



Managing Media Devices

Name: Managing Media Devices

Version: 1.3

Issue Date: 21/07/2008



File	Managing Media Devices	Pages	1	Version	1.3
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Document Control

This is a CONTROLLED document and updates or changes to this document are authorized and then advised by email to the relevant document holders.

It is UNCONTROLLED when printed. You should verify that you have the most current issue.

DOCUMENT HISTORY

Author(s)

Names	Role
John Pritchard	ICT Enterprise Architecture Manager

Document Log

Version	Status	Date Issued	Description of Change	Pages affected	Review
0.1	Draft		Creation of document		
0.2	Draft		Update	All	
0.3	Draft		Update	All	
0.4	Draft	21/07/2008	Released version for approval by IPG	All	
0.5	Draft	25/08/2008	Update	-	
0.6	Draft	26/08/2008	Update	-	
0.7	Draft	09/10/2008	Updated to reflect comments from consultation paper.		October 2008
1.0	Final	01/11/2008	Published	All	October 2009
1.1	Final	20/10/2008	Reviewed	All	October 2010
1.2	Final	05/10/2009	Reviewed	All	April 2011
1.3	Final	15/06/2011	Reviewed	All	May 2012

File	Managing Media Devices	Pages	2	Version	1.3
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Contents

Contents

1. Purpose	4
2. Scope.....	4
3. Breaches of Security	4
4. Encryption	5
5. Lost or Stolen Devices or Disks	5
6. Monitoring and Compliance.....	5
7. Leavers and Transfers	5
8. USB Memory Devices	5
9. CDs, DVDs Drives and Disks (Write or Rewrite)	6
10. Personal Digital Assistant (PDA)	6
11. Cameras	7
12. Mobile Phones, Smart phones and Blackberries	7
13. Roles and Responsibilities.....	7
14. Related Policies	8

File	Managing Media Devices	Pages	3	Version	1.3
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

1. Purpose

The purpose of this policy is to establish an authorised method for the use and control of mobile computing and storage devices that can contain or access information resources.

As mobile computing becomes more widely used, it is necessary to apply the appropriate security controls around these types of device and their use in order to protect the information resources of Herefordshire Council.

The aim is to enable users to use technology to carry out the tasks of their work, whilst taking into consideration the needs of the organisation to protect the data for which it is responsible.

2. Scope

This policy applies to all users of Herefordshire Council ICT systems, which may include (but is not exclusive to): Herefordshire Council employees, consultants, agency staff, contractors, Council Members, and all others who use mobile computing and storage devices on the Herefordshire Council network. These shall be referred to as 'users' throughout this policy.

This policy applies to mobile computing and storage devices which includes, but is not limited to: USB media (can also be known as memory sticks/flash sticks), CDs, DVDs, PDAs, digital cameras, portable hard drives, mobile phones, smart phones and blackberries. Within this policy each of these types of device or means of storage will have specific requirements, processes and responsibilities applied to them.

It is the policy of Herefordshire Council that all mobile computing and storage devices that can contain or access the information resources of Herefordshire Council must be approved prior to connecting to the information systems. This applies to all devices connecting to the Herefordshire Council network. Only media devices purchased through the ICT Procurement department may be used on the corporate network and under no circumstances are personal devices to be used. Written approval must be obtained from the Head of Services before confidential, sensitive or personal information is loaded to mobile computing or storage devices.

3. Breaches of Security

Any breach of this policy will be dealt with as set out in the "information security incident reporting procedure" which may lead to disciplinary action and possible termination of employment. Potentially illegal activities will be reported to the appropriate authorities.

File	Managing Media Devices	Pages	4	Version	1.3
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

4. Encryption

Mobile computing and storage devices can be easily lost or stolen, presenting a high risk for unauthorised access and introduction of malicious software to the network at Herefordshire Council. These risks must be mitigated to acceptable levels. Mobile computing devices and storage devices that contain confidential, personal, or sensitive Herefordshire Council information must be encrypted to ensure that the data is protected.

5. Lost or Stolen Devices or Disks

If at any time a user loses or has stolen from them any device or disk owned by Herefordshire Council this must be reported immediately to the ICT Helpdesk on 01432 260160 giving details of the make, model, HC asset number (if applicable) and the contents. ICT Services will then implement the ICT Incident Response process as outlined in the Information Security Incident Response Procedure document.

6. Monitoring and Compliance

ICT Services uses LANDesk on the network which is a software and hardware monitoring and compliance product. This will be used to ensure that users are able to use the various devices included in the scope of this policy, whilst at the same time providing security on these. LANDesk will be used to provide access to authorised equipment, prevent access to that which is unauthorised, monitor activity and provide encryption. Details of exactly how LANDesk will be used are included in each of the sections regarding the different types of devices and storage media.

7. Leavers and Transfers

Once a user either no longer has a business need for their authorised mobile device, they leave or change role within the organisation, their line manager will log an ICT helpdesk job, and ICT services will arrange for collection. Users must not pass these devices onto colleagues.

8. USB Memory Devices

In order to ensure that these devices are used securely by Herefordshire Council users, LANDesk will block the use of all devices other than those issued by ICT Services and will also be used to ensure that all data is securely held by encrypting the data.

File	Managing Media Devices	Pages	5	Version	1.3
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

To obtain a device users must have a clear work reason to use the device and should log a case with the ICT Helpdesk requesting a device giving details of the purpose for which it will be used and a cost code to cover the purchase cost. The request should detail the reasons and types of data that are to be used on the device. On receipt of the request an email will be forwarded to the user's Head of Service requesting confirmation that the device is required in order to carry out the tasks of the user's post and agreeing to the cost of the device. On receipt of confirmation, an email will be sent to the user asking them to carry out a short online training course and read an information guide. On successful completion of this the device will be issued by ICT Procurement.

Many third party companies and candidates attending interviews will want to use USB memory devices, this will not be possible without prior notification to the ICT Helpdesk - the user will be required to give the audit number of the computer or laptop on which the device is to be used together with the dates it is required, giving at least 24 hours' notice. On receipt of the request ICT Services will ensure that the use of USB memory devices is possible on nominated equipment for a defined period of time.

9. CDs, DVDs Drives and Disks (Write or Rewrite)

In order to ensure that these devices are used securely within Herefordshire Council, LANDesk will be used to block the use of all devices other than those issued by ICT Services and will also be used to ensure that all data is securely held by encrypting the data.

To obtain a device users must have a clear work reason to use the device and after seeking approval from their Head of Service, should prepare an ICT Request form for "Non-Standard Items" which is available on the intranet.

10. Personal Digital Assistant (PDA)

In order to ensure that these devices are used securely within Herefordshire Council, LANDesk will be used to block the use of all devices other than those issued by ICT Services.

To obtain a device users must have a clear work reason to use the device and should, after obtaining their Head of Service approval, prepare an ICT Request Form for Non-Standard Items which is available on the intranet.

File	Managing Media Devices	Pages	6	Version	1.3
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

11. Cameras

In order to ensure that these devices are used securely within Herefordshire Council, LANDesk will be used to block the use of all devices other than those issued by ICT Services.

To obtain a device users must have a clear work reason to use the device and should, after obtaining their Head of Service approval, prepare an ICT Request Form for Non-Standard Items which is available on the intranet.

12. Mobile Phones, Smart phones and Blackberries

In order to ensure that these devices are used securely within Herefordshire Council, LANDesk will be used to block the use of all devices other than those issued by ICT Services.

To obtain a device users must have a clear work reason to use the device and should, after obtaining their Head of Service approval, prepare an ICT Request Form for Non-Standard Items which is available on the intranet.

Users should also refer to the Corporate Telephone Usage Policy for full details.

13. Roles and Responsibilities

Heads of Service and Directors are responsible for informing ICT of any known media devices which are currently in use by their teams and reviewing requests for them.

Managers are responsible for informing their staff of this policy. They are responsible for any costs incurred from the misuse of these devices.

Users of media devices must ensure that they protect them from loss or damage and ensure that unauthorised disclosure of private and/or sensitive information belonging to or maintained by Herefordshire Council does not occur (further guidance on this can be sought from the ICT Information Security team). Unencrypted personal and sensitive data should not be stored on media devices. The ICT Helpdesk must be notified immediately upon detection of a security incident, for example when a mobile device may have been lost or stolen. To have ownership and responsibility of the data stored on the devices. This includes ensuring that any data subject to a request for information is made available in line with the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004, and that data is destroyed appropriately in line with the Council's retention schedules. Electronic documents should contain metadata and/or a document log identifying the Council as the copyright owner of the information. This must be enforced by managers.

File	Managing Media Devices	Pages	7	Version	1.3
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

The **Information Security Team** is responsible for the media device policy at Herefordshire Council and shall conduct a risk analysis to document safeguards for each media type to be used on the network or on equipment owned by the Herefordshire Council.

They are also responsible for developing procedures and monitoring best practice for implementing this policy.

They are responsible for any investigations of breach of this policy.

14. Related Policies

This policy is informed by and should be read in conjunction with, the following policies and procedures:-

- Corporate Information Security
- Corporate Telephone Usage
- ICT Incident Response Procedure
- Information Security Procedures
- Records Management Policy

File	Managing Media Devices	Pages	8	Version	1.3
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified